Math 373-578 **Name** _____

Homework Assignment 5
April 12, 2019

1. Use Pohlig-Hellman Algorithm to compute $\log_2(3)$ in $(\mathbb{Z}/53\mathbb{Z})^*$.
2. Find all the integer solutions to the congruence $x^{73} \equiv 614 \pmod{1159}$.
3. Alice and Bob are using RSA.
   (a) Bob's public key is $(N, e) = (899, 11)$. Alice wants to encrypt the plaintext 5. What does she send to Bob?
   (b) Suppose Eve discovers that $\phi(N) = 840$. How can she factor N?
   (c) If Eve intercepts the ciphertext 4 sent to Bob, what was the plaintext?